IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OHIO
EASTERN DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. BOGDAN NICOLESCU, et al. Defendant.	)))))))))))	CASE NO. 1:16-CR-224 JUDGE PATRICIA A. GAUGHAN REPLY IN SUPPORT OF UNITED STATES OF AMERICA'S SECOND MOTION *IN LIMINE* REGARDING AUTHENTICATION

Now comes the United States of America, by its counsel, Justin E. Herdman, United States Attorney, Duncan T. Brown and Brian M. McDonough, Assistant United States Attorneys, and Brian L. Levine, Senior Counsel for the U.S. Department of Justice, and hereby submits this Reply in Support of United States of America's Second Motion in Limine Regarding Authentication.

INTRODUCTION

As with the Government's hearsay motion, only Nicolescu has responded to the Government's authentication motion. Every issue Nicolescu raises in his opposition, however, goes to weight—not admissibility. These are arguments Nicolescu is free to raise with the jury, but they do not affect admissibility.

Nicolescu's brief reflects three fundamental misunderstandings regarding authentication:

First, Nicolescu argues (without any case support) that the Court should be "skeptical" of digital evidence because it can be "compromised," "impar[ed]," or "tampered with." Opp. at 3-4 and 8. But the Sixth Circuit has repeatedly said that the mere "possibility of tampering or misidentification" is not a basis for a court to preclude the admission of evidence. *United States*

v. Knowles, 623 F.3d 381, 386 (6th Cir. 2010) ("A party must do more than merely raise the possibility of tampering or misidentification to render evidence inadmissible."); *United States v. Combs*, 369 F.3d 925, 938 (6th Cir. 2004) (same); *United States v. Faulks*, 149 F.3d 1185 (6th Cir. 1998) (same). Further, FBI Computer Scientist Joe Corrigan is expected to testify that he reviewed the images of the digital devices and found no evidence of any activity occurring on the devices after the September 28, 2016 seizure, and thus no evidence of tampering. Dkt. 108 at 4. FBI Supervisory Special Agent Ryan MacFarlane is expected to testify similarly with respect to the RNP intercept data. *Id.* at 20.

Second, Nicolescu argues (also without any case support) that an unbroken chain of custody is "crucial" under the circumstances of this case. Opp. at 5. But the Sixth Circuit has made clear that "[g]aps in the chain affect the weight of the evidence and not its admissibility." *United States v. Fried*, No. 88-5292, 881 F.2d 1077, at *9 (6th Cir. Aug. 7, 1989); *see also Knowles*, 623 F.3d at 386 ("challenges to the chain of custody go to the weight of the evidence, not its admissibility.") (quoting *United States v. Levy*, 904 F.2d 1026, 1030 (6th Cir. 1990)); *Combs*, 369 F.3d at 938 (same).

Finally, Nicolescu misunderstands the concept of authenticating evidence through FRE 902(b)(4) ("distinctive characteristics"), repeatedly arguing that evidence should be excluded based on *how* it was located (i.e., through a "Google search" or through inexplicable Romanian internet intercepts). But like a cellphone happened upon in an empty field, we really don't need to know how it got there to figure out who it belongs to, if that can be shown through texts, emails, photos, or other "distinctive characteristics" associated with the item. (Dkt. 108 at 29.)

Below the government addresses the few "specific" objections raised by Nicolescu's opposition:

DISCUSSION

I. The Government Has Made a *Prima Facie* Case The Samsung Hard Drive Is Authentic

Despite offering no objection to the admission of two cellphones seized from his residence (the same location where the Samsung hard drive was seized), Nicolescu objects to the admission of the Samsung hard drive because he claims the government's asserted distinctive characteristic are too "tenuous", "circumstantial," "vague," and not "distinctive enough" to establish authenticity. Opp. at 7. In so arguing, however, Nicolescu minimizes the "distinctive characteristics," and ignores that the distinctive characteristics are offered *in addition to* substantial chain of custody evidence and other evidence the government intends to introduce.

A. Chain of Custody. The government will offer the testimony of at least three FBI witnesses who were part of the chain of custody for the Samsung hard drive. Dkt. 108 at 3. "FBI Supervisory Special Agent Ryan Macfarlane and FBI forensic agent Matthew Frost were both present at Nicolescu's residence during the [September 28, 2016] arrest and are expected to testify that the digital devices addressed below were found in Nicolescu's residence, placed in wax-sealed bags, and seized by Romanian law enforcement." *Id.* "FBI Special Agent Stacy Lough is expected to testify that on September 30, 2016, a Romanian prosecutor provided her with wax-sealed bags containing Nicolescu's digital devices and other seized evidence." *Id.* Thus, the only real gap in the chain of custody is the two day-gap between the time the RNP took custody of the *wax-sealed* bags of evidence and presented those *still-sealed* bags to Special Agent Lough on September 30. *Id.* Yet FBI Computer Scientist Joe Corrigan will testify that he reviewed the images of the digital devices and found no evidence of any activity occurring on the devices after the September 28, 2016 seizure, and thus no evidence of tampering. *Id.* at 4. The Sixth Circuit has made clear that "[g]aps in the chain affect the weight of the evidence and

not its admissibility." *Fried*, No. 88-5292, 881 F.2d 1077, at *9; *Knowles*, 623 F.3d at 386; *Levy*, 904 F.2d at 1030; *Combs*, 369 F.3d at 938.

B. Found with Already Authenticated Evidence. In addition to the chain of custody evidence described above, the Samsung hard drive was found in Nicolescu's residence—the same location as two cellphones that Nicolescu concedes are authentic. All three devices are listed on the inventory form that Nicolescu signed. *See* Govt. Ex. 5. The Court can consider that inventory pursuant to FRE 104(a), whether or not it is admitted as an "adopted admission." Numerous judicial opinions show that the fact that one item in a particular location is determined to be *prima facie* authentic helps establish the authenticity of other items located in the same location. Dkt. 108 at 38 n.15.

C. Distinctive Characteristics. The fact that, in his motion, Nicolescu describes this evidence in a vague and nondescript manner does not somehow make the evidence vague or nondescript. The government pointed out that the Samsung hard drive contains an invoice emailed to Tzolea@yahoo.com—an account demonstrably associated with the Bayrob Group. Dkt. 108 at 5. The hard drive also contains at least five programs routinely used by the Bayrob Group (and found on the devices of the other defendants), including TrueCrypt (an encryption program), TOR (an anonymized network), Pidgeon OTR (the software the Bayrob Group used for encrypted chat), PGP encrypted email files (PGP is the software the Bayrob Group used for encrypting emails), proxy programs (to tunnel traffic through other computers), and wrt54gl.rar (a program that the Bayrob Group used to tunnel traffic through stolen wireless access points). Dkt. 108 at 5-6. The information on the hard drive was also consistent with the information on both phones (which Nicolescu concedes are authentic), including the use of Pidgeon OTR, further bolstering authentication. *Id.*

D. Co-Conspirator Testimony. Nicolescu may find that this "distinctive characteristic" evidence is "vague," but Tiberiu Danet and other Bayrob associates are expected to testify that Nicolescu was MasterFraud—the leader of the Bayrob Group—and that the "vague" items found on the Samsung hard drive were used by Nicolescu as part of his criminal scheme leading the Bayrob Group. Dkt. 108 at 37.

Under Sixth Circuit law, this is more than sufficient to make a *prima facie* case.

II. The Government Has Made a *Prima Facie* Case that the RNP Intercepts and Screenshots are Authentic

The government addresses Nicolescu's argument regarding the RNP intercepts and screenshots together because both arguments suffer from the same fundamental flaw. Nicolescu mistakenly believes that *prima facie* authentication of evidence always depends on "how" the evidence is located and recovered. As discussed extensively in the government's motion (Dkt. 108 at 27), establishing "how" evidence is located and recovered may be necessary where the evidence is "non-distinct," such as cocaine. *See United States v. Cardenas*, 864 F.2d 1528, 1531 (10th Cir. 1989) ("Cocaine, [which is] not uniquely identifiable, requires a sufficient chain of custody to support its admission."). It is not necessary, however, where the evidence is, itself, distinct—as is frequently the case with digital evidence. *See Lorraine v. Markel*, 241 F.R.D. 534, 546-48 (D. Md. 2007) (describing FRE 901(b)(4) ["distinctive characteristics"] as "one of the most frequently used [rules] to authenticate email and other electronic records."). In contrast to the government's mountain of authority supporting authentication of digital evidence based on "distinctive characteristics" (e.g., Dkt. 108 at 32-38), Nicolescu cites no authority to support his position that this common method is inappropriate.

A. Screenshots. Guided by this mistaken premise, Nicolescu criticizes the web posts the Government seeks to authenticate solely because of how they were found—"through a

'Google' search." Opp. at 8. Nicolescu argues that a "Google search" is "outside the means of accepted methodology for authenticating evidence." *Id.* But the government does *not* seek to authenticate the evidence *because* it found it through a Google search. The government seeks to authenticate the posts as posts created by Miclaus based on the "distinctive characteristics" of the posts themselves.

Regardless of how they were found, the government presented overwhelming evidence (more than sufficient for a *prima facie* case) that each of these three posts was personally created by Radu Miclaus, and is thus relevant and admissible. Dkt. 108 at 23-25. As an example, the Twitter post (Ex. 1448) was clearly created by Miclaus because, among other things, Miclaus' Huawei phone shows that Miclaus controlled this exact Twitter account, and because the exact same skydiving photo in the Twitter post was also found on Miclaus' Huawei phone (Ex. 214), his Samsung phone (Ex. 301), and on surveillance of his home internet (Ex. 1941). *Id.* at 23-24. Further the government witnesses who visited these websites and took these screenshots will testify at trial that they visited these websites, took these screenshots, and that the exhibits are fair and accurate representations of what they saw on the web. *Id.* Nothing more is required. *Id.* at 32-38. Miclaus (who has not opposed the government's motion)[1] is free to argue that he did not create the posts, but the government has presented *prima facie* evidence that he did, regardless of how that evidence was located.[2]

---

[1] Given that the government has offered these screenshots as web posts created by Miclaus, if Miclaus does not contest the authenticity of these posts, Nicolescu should not be permitted to contest their authenticity.

[2] Nicolescu incorrectly maligns these screenshots as representing the government "throwing everything it can find [at the case] regardless of how tenuous and remotely circumstantial." Opp. at 8. To the contrary, the evidence at trial will show that this exact open-source research was a key step that led to identification of the Bayrob Group.

B. RNP Intercepts. The analysis of the RNP intercepts is no different than the analysis of the screenshots. Although the government intends to introduce testimony from former members of the RNP about how they reliably obtain such internet interceptions and testimony from FBI agents that they formally requested and received this evidence in the expected form with no evidence of tampering—the intercepts are primarily authenticated by the "distinctive characteristics" of the intercepts themselves. *Id.* at 20-23. For example, the RNP surveillance identified OTR-encrypted instant messages from Nicolescu's wbw.bogdan account to tibi_danet. *See, e.g.*, Exs. 1932. Nicolescu does not contest the authenticity of his phones (Opp. at 6), which phones show that Nicolescu controlled the wbw.bogdan account. *See, e.g.*, Exs. 29-31, 37, 55-56, 160-61. Further, Danet (tibi_danet) will testify that wbw.bogdan was an account used by Nicolescu and that he had OTR-encrypted chats with Nicolescu using that account. That is more than sufficient for *prima facie* authentication.

Nicolescu argues that he "specifically objects" to the surveillance records that show "numerous encrypted chats" over Defendant Danet's Jabber server because "Danet could have tampered with" them. Opp. at 8. But again, the Sixth Circuit is clear that the mere "possibility of tampering or misidentification" is not a basis for a court to preclude the admission of evidence. *Knowles*, 623 F.3d at 386 ("A party must do more than merely raise the possibility of tampering or misidentification to render evidence inadmissible."); *Combs*, 369 F.3d at 938; *Faulks*, 149 F.3d 1185. Moreover, Nicolescu will be free to cross examine Danet at trial as to whether he "tampered with" his own server to create incriminating records between himself and Nicolescu.

CONCLUSION

In order to streamline the trial and reduce jury confusion, the United States respectfully requests that the Court grant its Second Motion *in Limine* Regarding Authentication and rule that the digital devices seized from the defendants or their residences (and thus, the evidence found thereon), Romanian internet intercepts, and three screenshots are *prima facie* authentic.

Respectfully submitted,

JUSTIN E. HERDMAN
United States Attorney

By: /s/ Brian L. Levine

Brian L. Levine (DC: 480216)
Senior Counsel
United States Department of Justice
1301 New York Avenue, Suite 600
Washington, DC 20005
(202) 616-5227
(202) 514-6113 (facsimile)
Brian.Levine@usdoj.gov

Duncan T. Brown (NY: 3982931)
Assistant United States Attorney
United States Court House
801 West Superior Avenue, Suite 400
Cleveland, OH 44113
(216) 622-3933
(216) 522-7499 (facsimile)
Duncan.Brown@usdoj.gov

Brian M. McDonough (OH: 0072954)
Assistant United States Attorney
United States Court House
801 West Superior Avenue, Suite 400
Cleveland, OH 44113
(216) 622-3965
(216) 522-2403 (facsimile)
Brian.McDonough@usdoj.gov

CERTIFICATE OF SERVICE

I hereby certify that on this 17th day of February, 2019, a copy of the foregoing Reply in Support of Government's Motion on Authentication was filed electronically. Notice of this filing will be sent to all parties by operation of the Court's electronic filing system. Parties may access this filing through the Court's system.

/s/ Duncan T. Brown
Duncan T. Brown
Assistant United States Attorney